Aprobado en Consejo Informático 19-3-2013

PROTOCOLO DE BLOQUEO DE CUENTAS COMPROMETIDAS

Introducción

El objetivo de este documento es presentar una propuesta para un protocolo de bloqueo de cuentas comprometidas en las que se pueda constatar un uso ilegítimo de las mismas.

Los riesgos que una cuenta atacada genera para la institución y el propietario son:

- En cuanto al ámbito de los servicios afectados:
  - Envíos de mensajes de correo electrónico no solicitados (spam) desde la cuenta afectada.
  - Acceso ilegítimo a servicios corporativos (Campus Global, aplicaciones de docencia, gestión de personal, etc.), permitiendo al intruso desde modificar unas notas hasta cambiar la cuenta bancaria de destino de la nómina.
- En lo relativo al impacto que tiene una cuenta comprometida:
  - El perjuicio inmediato es para la institución, en dos facetas, la primera es la imagen corporativa, ya que puede ser considerada una organización emisora de correo no deseado y ser incluida en varias de las numerosas listas negras de spam que existen en la red. Por otra parte todos los usuarios de la universidad se ven afectados, ya que la inclusión en listas negras implica que no se pueda entregar correo a las instituciones que utilizan estas listas para filtrar su correo entrante. Por ejemplo, si entramos en una lista negra que utiliza Google todos los correos de la universidad dirigidos a Gmail serían rechazados.
  - También el titular de la cuenta comprometida se ve afectado, ya que su correo está a disposición del intruso, además de todos aquellos servicios de red que utilizan la cuenta de servicios corporativos (Campus Global, Aula, Portal del Empleado, y otros servicios específicos del usuario). Adicionalmente se ve perjudicada la "imagen en internet" del titular de la cuenta comprometida, pudiendo sufrir bloqueos de su dirección. Además si el intruso obtiene acceso a su perfil en redes sociales, puede realizar publicaciones en su nombre.

Bases de la propuesta

Dentro de las funciones del Servicio de Informática está el velar por el correcto uso y funcionamiento del Correo Electrónico (basado en el artículo 9 del Reglamento del Servicio de Informática).

Estas situaciones de compromiso de cuentas corporativas, como se ha visto, suponen un serio perjuicio tanto para el usuario afectado como para el resto de la comunidad universitaria. Se hace necesario el uso de algún procedimiento que permita atajar la situación en el menor tiempo posible, minimizando el impacto que pueda tener sobre el acceso a los servicios corporativos por parte del usuario.

Ámbitos de aplicación

Recaerán dentro del ámbito de este procedimiento todos aquellos casos en los que se confirme que una cuenta ha sido comprometida.

La detección de estos casos la realizará el Servicio de Informática y Comunicaciones, que será el responsable de poner los medios necesarios para una precoz identificación de la cuenta afectada así como del tipo de uso que se esté haciendo de ella.

Procedimiento de bloqueo

Una vez identificado una cuenta comprometida, el Servicio de Informática y Comunicaciones procederá según las siguientes fases:

Fase 1: Identificación de la persona vinculada a la cuenta comprometida

A través del directorio de la universidad, o del servidor LDAP se localizará la persona responsable de la cuenta ha sido comprometida.

Fase 2: Notificación al usuario responsable de la cuenta

Dado que una vez que se haya bloqueado la cuenta, no se tendrá acceso al correo, se tratará de contactar con el titular utilizando los métodos disponibles:

- Por teléfono, se realizará una llamada a la extensión corporativa (previamente localizada en el directorio). Si no fuera posible contactar con el interlocutor, se dejaría un mensaje informativo en el contestador.
- En caso de que el servicio de correo electrónico estuviera redirigido a un servidor externo, el Servicio de Informática enviará un mensaje informativo a la cuenta destino de dicha redirección.
- También se enviará una copia de dicho mensaje a:
    - Secretaría del departamento.
    - Centro de Atención a Usuarios (caso@uc3m.es), para que tengan constancia del bloqueo.
    - Representante en el Consejo Informático del departamento al que pertenezca el usuario.
- Si se trata de un usuario con cargo institucional se tratará de localizar a la secretaria asociada, para que localice al usuario a la mayor brevedad posible.

Fase 3: Bloqueo de la cuenta comprometida

Si no se ha conseguido localizar al usuario, una vez cumplidos los pasos anteriores y pasado el plazo de una hora, se procederá al bloqueo de la cuenta.

Si el uso que está haciendo de la cuenta el intruso es únicamente el envío de mensajes a través de las estafetas de correo de la universidad, valiéndose de la autenticación SASL (el que utilizan los programas de correo como Outlook o Thunderbird), se procederá al bloqueo de esta funcionalidad, de forma que no se podrán enviar correos desde dichos programas o cliente de correo de dispositivos móviles. Sí se podrá consultar el correo desde cualquier dispositivo, aunque el envío de mensajes sólo se podrá realizar a través del WebMail .

A partir de este momento, la cuenta comprometida no podrá ser utilizada para enviar mensajes, aunque se podrá acceder a los servicios corporativos (correo, Campus Global, eduroam, VPN, etc.)

Si el intruso está realizando envíos a través del Webmail corporativo o accediendo a otros servicios corporativos (calificaciones, gestión de personal, etc.), la medida anterior no resulta eficaz, siendo necesario proceder al bloqueo de la cuenta del usuario.

En este caso la cuenta bloqueada no podrá ser utilizada para acceder a ningún servicio corporativo.

Fase 4: Cambio de contraseña

El propietario de la cuenta deberá realizar un cambio de contraseña, mediante los mecanismos previstos para la situación en la que no se recuerda la contraseña actual. Más información en:
http://www.uc3m.es/portal/page/portal/informatica/NosDedicamos/ServiciosCorporativos/CorreoElectronico#cambio

Fase 5: Eliminación de la restricción

Una vez cambiada la contraseña, la cuenta volverá a ser completamente operativa.

Anexo: Diagrama de flujo bloqueo de cuenta comprometida